REMARKS

The Examiner maintains the primary rejection of the claims based on Song.. Reconsideration and allowance are requested.

The question is whether the way in which Song selects execution units can reasonably be interpreted to be pseudo random under the current law regarding claim construction. Applicant respectfully submits that the answer is no.

The Examiner on page 10 asserts that events such as asynchronous interrupts and user inputs in Song satisfy the claimed features relating to the "pseudo random execution mechanism selecting signal." The Examiner indicates that the feature of the pseudo random signal generator should be interpreted by giving the words their plain meaning. This is not a complete rendering of the proper legal standard for claim construction by the USPTO. The Federal Circuit has held on several occasions that a plain and ordinary claim term interpretation must be consistent with the understanding one of ordinary skill in the technical field would have in the context of the application. "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). See also *In re Cortright*, 165 F.3d 1353, 1359 (Fed. Cir. 1999)(The broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach). The MPEP §2111 similarly mandates:

> The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "**in light of the specification as it would be interpreted by one of ordinary skill in the art.**" *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004).

A person of ordinary skill in the field of secure microprocessor design would not have considered the asynchronous interrupts and user inputs referred to by the Examiner as being pseudo random signals in light of the specification of this application.

The technology described in claims 1 and 14 provides protection against security attacks based upon timing analysis and power analysis. As explained in the specification, by observing the time behavior and/or the power consumption behavior of the system in response to inputs, information concerning the processing performed and the data being manipulated can be determined in a way that compromises security. The pseudo random selection of the different execution mechanisms as claimed resists these types of timing analysis and power analysis attacks.

The kind of external signals referred to by the Examiner, including interrupts and inputs received from a user, would not have been understood by a skilled person in this art as pseudo random. Rather, that skilled person would have understood that a linear feedback shift register of the type disclosed in the example of Figure 7 of the current application is one known non-limiting way to generate a pseudo random signal. In fact, interrupts and inputs received from a user are the very type of inputs which may well be used in timing and power analysis attacks. By manipulating these inputs and performing a statistical analysis, it is possible to identify underlying behavior in a manner which is not masked by the execution mechanism selection. Thus, the skilled person reading Song would not consider asynchronous inputs and user inputs to be pseudo random signals as claimed, but would instead regard them as non-random signals capable of manipulation and statistical analysis in a manner which would permit a security "crack."

The independent claims have been amended to clarify that the pseudo random selection is independent of external inputs to the apparatus such as the unpredictable behavior mentioned by the Examiner relating to external inputs. Moreover, amended claims 1 and 14 make clear that the pseudo random generator is part of the apparatus and that the pseudo random execution mechanism selecting signal is generated within the apparatus.

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100